Swami Ramanand Teerth Marathwada University, Nanded
Ph.D. (Computer Science): Synopsis

Name of Research Scholar: Mr. Patil Pratap Paraji
Mobile No.: 09822538753 / 09579209440
Email: pratapmcs@gmail.com
Category: Open.
Physical Handicapped: No.
Research Center: Swami Vivekanand Mahavidyalaya, Udgir, Latur.

Name of Research Guide: Dr. Jagtap Sudhir Baburao
Principal, Swami Vivekanand Mahavidyalaya, Udgir, Latur.
Mobile No.: 09422611355.
Email: sudhir.jagtap7@gmail.com

Faculty: Computer Studies
Subject: Computer Science
Research Topic: “A hybrid approach to enhance security and protect Multi-model Biometric templates.”

A Hybrid Approach to Enhance Security and Protect Multi-model Biometric Templates

Submitted to

Swami Ramanand Teerth Marathwada University, Nanded.

for the partial fulfillment of
award of Ph.D. degree in Computer Science

By
Mr. Pratap P. Patil

Under the Guidance of
Dr. Jagtap Sudhir Baburao
Principal,
Swami Vivekanand Mahavidyalaya, Udgir.

June 2016

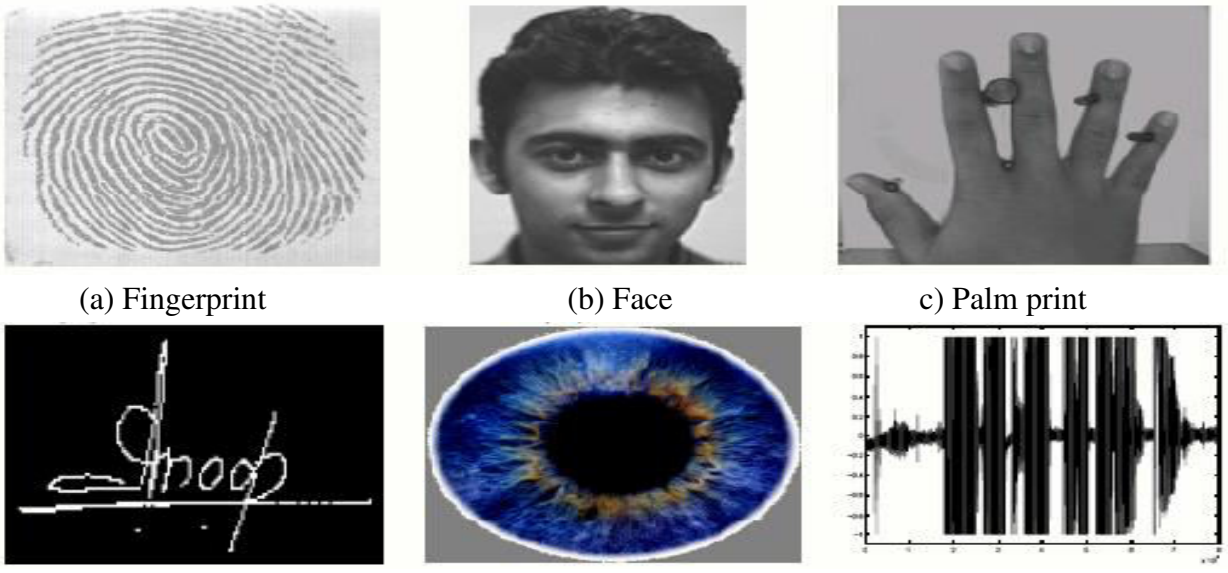
1. Introduction:

A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else. Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor.

Traditionally, passwords (knowledge-based security) and ID cards (token- based security) have been used to restrict access to systems. However, security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user). The emergence of biometrics has addressed the problems that traditional verification methods.

Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess (e.g. an ID card) or what you remember (e.g. a password).

Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, face, signature, voice, gait, palm print, etc. (Figure 1.1) to establish a person's identity. While biometric systems have their limitations, they have an edge over traditional security methods in that it is significantly difficult to lose, steal or forge biometric traits; further, they facilitate human recognition at a distance (e.g. face and gait).



(a) Fingerprint (b) Face c) Palm print

(d)Signature e) Iris (f) Voice

Figure 1.1: Some examples of the biometric traits used for authenticating an individual.

Biometric systems also introduce an aspect of user convenience that may not be possible using traditional security techniques. For example, users maintaining different passwords for different applications may find it challenging to recollect the password associated with a specific application. In some instances, the user might even forget the password, requiring the system administrator to intervene and reset the password for that user. Maintaining, recollecting, and remembering passwords can, therefore, are a tedious and

expensive task. Biometrics, on the other hand, addresses this problem effectively, thereby enhancing user convenience: a user can use different passwords (biometric traits) for different applications, with password recollection not being an issue at all.

A typical biometric system operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template feature set in the database. In the following figure 1.2, an identification scheme the comparison is done against templates corresponding to all the enrolled users in order to recognize the individual (a one-to-many matching); in a verification scheme, the comparison is done against only those templates corresponding to the claimed identity in order to verify the claim (a one-to-one matching). Thus, identification (Whose biometric data is this?) and verification (Does this biometric data belong to XYZ?) are two different problems with different inherent complexities. The templates are typically created at the time of enrollment, and depending on the application may or may not require human personnel intervention.

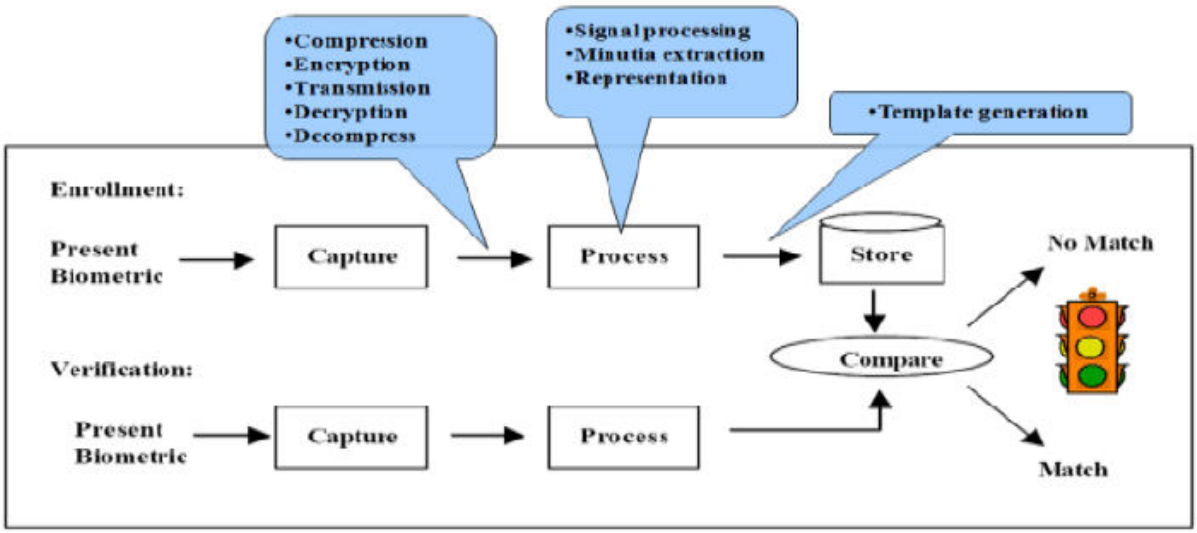


Figure 1.2: The enrollment module and the verification module of a biometric system.

- Biometric system modules:

1. Sensor Module which captures the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a user.
2. Feature Extraction Module in which the acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint image would be computed in the feature extraction module of a fingerprint system.
3. Matching Module in which the feature values are compared against those in the template by generating a matching score. For example, in this module, the number of matching minutiae between the query and the template can be computed and treated as a matching score.
4. Decision-making Module in which the user s claimed identity is either accepted or rejected based on the matching score generated in the matching module (verification).

The biometric authentication system uses two kinds of approaches- (Figure 1.3) Uni-modal and Multimodal. Biometric systems used in real world applications are uni-modal. These uni-modal biometric systems rely on the evidence of a single source of information for authentication of person. A uni-modal biometric system has sensor module to capture the

trait, feature extraction module to process the data to extract a feature set that yields compact representation of the trait, classifier module to compare the extracted feature set with reference database to generate matching scores and decision module to determine an identity or validate a claimed identity. Though these uni-modal biometric systems have many advantages, it has to face with variety problems like: Noise in sensed data, biometric data can be contaminated by noise due to imperfect acquisition conditions which may lead to false rejections. Intra class variation, the biometric data acquired during verification will not be identical to the data used for generating template during enrollment for an individual. This is known as intra class variation. Large intra-class variations increase the False Rejection Rate (FRR) of a biometric system. Interclass similarities, the overlap of feature spaces corresponding to multiple individuals. Large Inter-class similarities increase the False Acceptance Rate (FAR) of a biometric system. These problems were addressed by introducing multimodal biometric approach. It consolidates multiple sources of biometric information. This can be accomplished by fusing. Fusion can be done at different levels like Sensor level fusion, this fusion refers to the consolidation of raw data obtained using multiple sensors or multiple snapshots of biometric using a single sensor. Feature level fusion, this fusion refers to the consolidation of features sets from different biometric traits into single feature set of features. Score level fusion, in this level of fusion, the match scores output by multiple matchers are combined to generate a new match score that can be subsequently used by verification or identification modules for rendering an identity decision. Decision level fusion, this fusion combines multiple decisions.

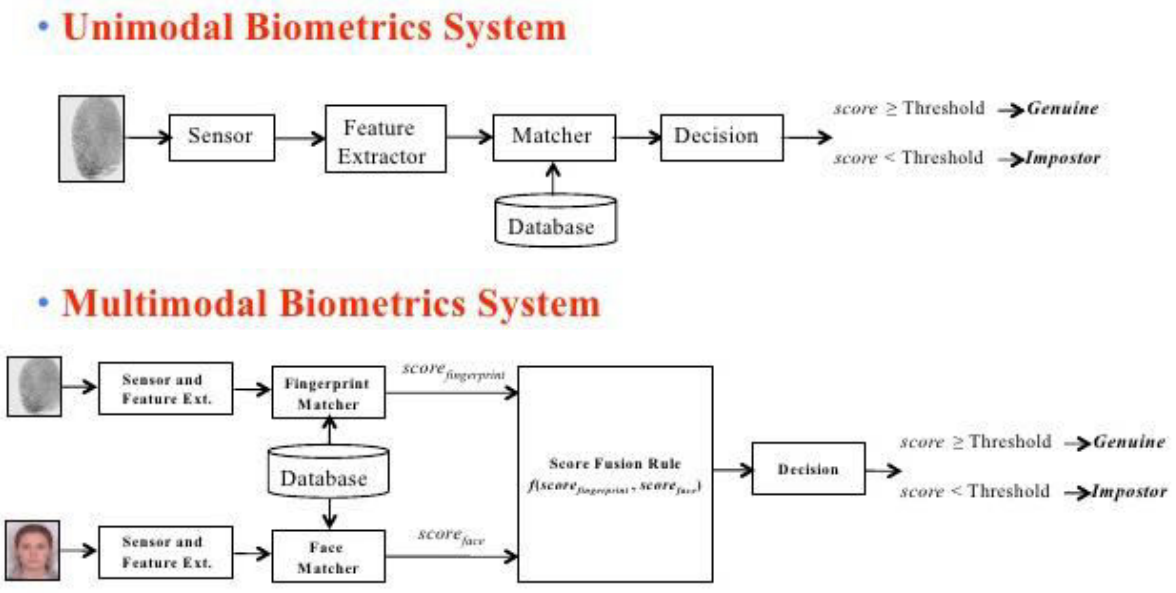


Figure 1.3: Uni-modal and Multi-modal Biometric systems

- Biometric Templates:

A template represents a set of salient features that summarizes the biometric data (signal) of an individual. A biometric template is a digital reference of distinct characteristics that have been extracted from a biometric sample. Templates are used during the biometric authentication process. Due to its compact nature, it is commonly assumed that the template cannot be used to elicit complete information about the original biometric signal.

Furthermore, since the templates are typically stored in an encrypted form, it is substantially difficult to decrypt and determine the contents of the stored template.

- Constraints for Biometric Templates:

Protected biometric templates used in privacy -protected verification system should satisfy the following constraints;

- Original biometric samples should not be decoded from the protected templates.
- Private information should not be derived from the protected templates.
- It should not be possible to link subjects within and across the databases through comparison of templates.
- Should allow identity verification data for specific predefined application only.

- Application Areas of Biometrics:

Biometric authentication finds its applications in the following vital areas namely**:**

- Access Control to Facilities and Computers.
- Criminal Identification.
- Border Security.
- Access to Nuclear Power Plant.
- Identity Authentication in Network Environment.
- Airport Security.
- Issue of Passports or Driving Licenses.
- Forensic and Medical Databases.

- Attacks against Biometric Systems:

Biometric systems are prone to a variety of attacks. Attacks against biometric systems are grouped into four categories namely,

1) Attacks at the user interface (input level),
2) Attacks at the interfaces between modules,
3) Attacks on the modules,
4) Attacks on the stored templates.

Among the above four varieties of attack, the stored Biometric Template Attack is the worst. This research work provides security to Biometric Templates against stored biometric template attacks.

- Need for biometric template security:

As biometrics finds its applications in crucial high security areas and is subjected to different types of attacks, providing security and revocability to the biometric template is an important issue. Biometrics is not private and only limited biometrics are present in the human body. Hence, it is very important to secure biometric templates. Moreover, they leak personal information like disease and disorders in a person. When the biometric is lost, a person loses his identity. Therefore providing security to biometric templates is very important in any biometric based authentication system. (See Figure 1.4)

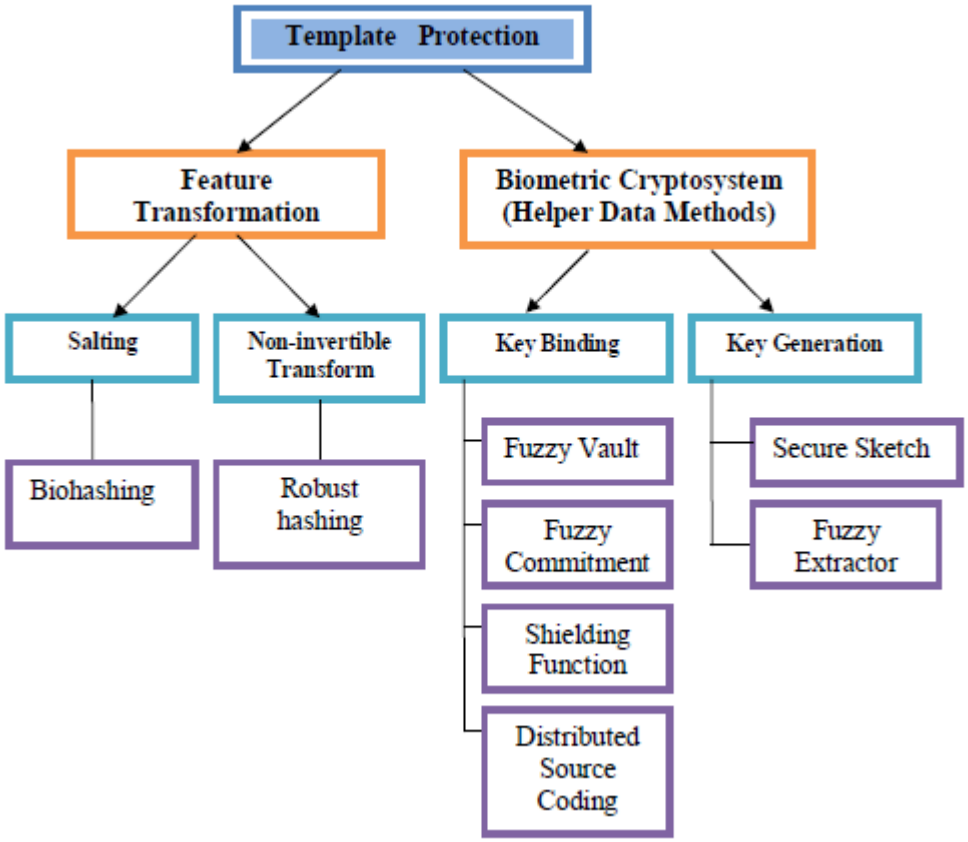


Figure 1.4: Categories of Biometrics Template Protection Methods

A) Feature Transformation Based Methods:

A transformation function (F) is designed using the key generated from the random key (K) or password. The biometric template is transformed by applying the transformation function. The transformed template (F (T, K)) is stored in the database. Similarly the Query template (Q) is also transformed using the same transformation function. The transformed Query template (F (Q, K)) is compared with the transformed template F ((T, K)). Based on the transformation function F, the transformation schemes are further classified as salting and non-invertible transforms.

(i) Salting:

The user password or random numbers are mixed with biometric information. These user specific factors are used to obtain a transformed or changed copy of a biometric template. To provide revocability, this user specific component can be changed to obtain another new copy of the biometric template.

(ii) Non-invertible transformation:

The non-invertible methods apply one-way function on the biometric template. Even if the key is gained, it is computationally hard to invert a transformed template. In this approach, the biometric template is secured by applying a non-invertible transformation function to it. Non-invertible transform refers to a one- way function, F, that is "easy to compute" (in polynomial time) but "hard to invert" (given F(x), the probability of finding x in polynomial-time is small).

B) Biometric Cryptosystems:

Biometric Cryptosystem based methods blend the idea of both biometrics and cryptography. They are initially used to protect cryptographic key by using biometric information. They are also used to generate cryptographic keys from biometric features. However, they can also be used for template protection. These methods involve public information known as helper data about the stored templates. Helper data does not leak any significant information about the original biometric template. Biometric cryptosystem based methods are also called Helper Data Based Methods. Helper data is utilized to extract cryptographic key from the query biometric features. Validity of the extracted key checked during matching.

Error correction coding techniques are typically used to handle intra-user variations. Biometric cryptosystem are further classified into key binding and key generation based methods.

(i) Key Binding Based Methods:

When the helper data is obtained by binding a key with the biometric template, then it is referred as a key-binding biometric cryptosystem. In a key binding cryptosystem, the biometric template is secured by binding it with a key within a cryptographic framework. A single entity that embeds both the key and the template is stored in the database as helper data. This helper data does not reveal much information about the key or the biometric template, i.e. it is computationally hard to decode the key or the template without any knowledge of the user's biometric data. Recovery of the correct key implies a successful match.

a) Fuzzy Vault:

This construct is more suitable for applications where biometric authentication and cryptography are fused together. Fuzzy vault framework, thus utilizes the goodness of both cryptography and biometrics. In fuzzy vault framework, the secret key S is locked by G, where G is an unordered set from the biometric sample. A polynomial P is constructed by encoding the secret S. This polynomial is evaluated by all the elements of the unordered set G. A vault V is constructed by the union of unordered set G and chaff point set C which is not in G, i.e. $V = G \cup C$.

b) Fuzzy Commitment:

Fuzzy commitment technique was proposed by Juels and Wattenberg. They combined the error-correcting codes and cryptography to fuzzy commitment scheme. By contrast, our scheme is fuzzy in the sense that it accepts a witness that is close to the original encrypting witness in a suitable metric, but not necessarily identical.

c) Shielding function and Distributed Source coding:

This method is proposed to prevent misuse of the biometric information from the system administrator. The acquired biometric information is subjected to delta-contracting and epsilon-revealing function. As a result of this the biometric template becomes computationally hard to trace back the original information of the individual. This idea is similar to fuzzy extractors.

(ii) Key Generation Based Methods:

If the helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features, it leads to a key generation biometric cryptosystem. Direct cryptographic key generation from biometrics is an attractive proposition but it is a difficult problem because of the intra-user variability.

a) Fuzzy Extractor:

A fuzzy extractor reliably extracts nearly uniform randomness 'R' from its input. The extraction is error-tolerant in the sense that 'R' will be the same even if the input changes, as long as it remains reasonably close to the original. Thus, 'R' can be used as a key in a cryptographic application.

b) Secure Sketch:

A Secure sketch reliably reproduces the biometric secret without leaking any information. A sketch scheme consists of two parts. The first part of the algorithm is a sketch generation algorithm Gen. The second part of the algorithm is a reconstruction algorithm Rec. Given some data X, the output Px = Gen(X) is called a sketch of X. Given a sketch Px and another Y that is sufficiently similar to X according to some measure, Rec(Px, Y) would reconstruct the original X.

2. Review of Literature and Development in the subject:

A single approach is not enough to achieve all the properties of a biometric template like security, revocability and diversity. Multi-biometrics are more significant than uni-biometric systems as they overcome certain limitations of uni-biometrics. Multi-biometric authentication systems are employed in several high security applications providing security to Multi-biometric system is of much importance.

The limited security of multimodal recognition systems, the drawbacks of biometric template protection technologies and the major absence of practicality to the recognition algorithms, involved in these creations, have motivated researchers to examine the possibilities for a fortunate combination of the two areas. The relation between biometrics and protection techniques brings new challenges and illustrates efforts for further scenarios which can promise better overall accuracy of the system.

Literature survey has revealed a number of experimental works or approaches that are focused on the most frequently used biometrics (iris, finger print, face pattern etc) and aim at reducing the errors and providing higher security.

- Christina-Angeliki Toli, Bart Preneel [2015] have presented a concrete approach on the protection of multimodal biometric templates, underlying critical privacy issues, while focusing on the suggestions for future research. Multimodal biometric systems are mostly discussed for the impact of their use on publicly accepted, reliable identification systems, overcoming the obstacles of uni-modal ones.
- Praveer Tigga, Akash Wanjari, [2015] states the limitations of the single characteristic as a verification tool are revealed, while the vitality of multimodalities against fraudulent technologies is under examination. While biometric vendors are deploying multi

biometric systems, at the same time concerns arise from the storage and misuse of the data. The security of the templates is especially crucial for the confidentiality and integrity of this sensitive information. In the direction of facing a number of threats, works on the two main categories of biometric template protection schemes offer important advantages. The incorporation of multiple biometrics in template protection schemes seems that can offer suggestions for solution against many drawbacks, while new security interrogations arise.

- Jialiang Peng; Qiong Li; Ahmed A. Abd El-Latif et al [2014] addresses two critical issues in the design of a finger multi-biometric system, i.e. fusion strategy and template security. First, three fusion strategies (feature-level, score-level, and decision-level fusions) with the corresponding template protection technique are proposed as the finger multi-biometric cryptosystems to protect multiple finger biometric templates of fingerprint, finger vein, finger knuckle print, and finger shape modalities. Second, we theoretically analyze different fusion strategies for finger multi-biometric cryptosystems with respect to their impact on security and recognition accuracy.
- G. Karthi, M. Ezhilarasan, [2013] states that protecting Biometric Template has increasingly gained popularity. Researcher proposes a hybrid technique, which uses Biometric Cryptosystems and Feature Transformation. In Feature Transformation, if the user specific token is theft means the template is no longer safe. The Experimental Results shows no degradation in FAR & FRR by combining both the Biometric Cryptosystem and Cancelable Biometrics.
- Shweta Malhotra, Chander Kant Verma, [2013] introduced an approach which includes multimodal biometrics and also key binding which helps to keep the templates secure and uniquely identify a person. With these two concepts the approach is called hybrid and can be used to accurately identify an individual. There are many multimodal biometric systems in existence for authentication of a person but still selection of appropriate modals, choice of optimal fusion level and redundancy in the extracted features are some challenges in designing multimodal biometric system that needs to be solved.
- The work of L. Nanni, E. Maiorana, A. Lumini and P. Campisi [2010] focuses on an on-line signature authentication system based on an ensemble of local, regional, and global matchers. The template protection scheme employing the Bio-Hashing and the Bio-Convolving approaches, the two well known template protection techniques for biometric recognition, are discussed.
- A. Nagar, K. Nanda Kumar, and A. K. Jain [2010] conclude that encrypted polynomial evaluations of fuzzy vault using fuzzy commitment scheme. Due to this the vault cannot be gained even if the genuine points are captured. They proposed a hybrid scheme by mixing the idea of fuzzy commitment and fuzzy vault scheme.

3. Objectives of Research:

- To enhance the security of the multi-model biometric systems using hybrid approach.
- To make biometric templates more resistive to biometric template attacks.
- To utilize the idea of multi-model biometrics to overcome certain limitations of uni-model biometrics system.

Research Question:

Multi-model Biometric template protection is very important to answer a crucial question: "*How can the leakage of stored biometric characteristics, to unauthorized individuals, be prevented?*"

Scope of Study:

This proposed study will cover enhancement of the performance and security of a multi-model biometric system using fingerprint, face, Iris, signature traits etc of a subject. The proposed system will cover hybrid approach to protect Biometric Template consisting of 2 categories of Biometric Template protection i.e. Feature Transformation and Biometric Cryptosystems.

4. Methodology to be adopted:

A number of techniques have been designed to improve the security of biometric templates. The hardware based approach involves designing a "closed" recognition system, where the biometric template never leaves a physically secure module such as a smart card or a hand-held device. The card or device may contain only the template and the matcher (Match-on-card) or the complete biometric system including sensor, feature extractor, template, and matcher (System-on-card). Such a device matches the input biometric trait with the template stored in the device and releases a key in case the authentication is successful.

Software-based solutions for template protection store a modified version of the template that reveals as little information about the original biometric trait as possible and yet can be successfully used for authentication. The template protection can be classified into two main categories: (i) Template or Feature Transformation, (ii) Biometric Cryptosystem.

- Template transformation techniques transform the biometric template based on parameters derived from external information such as user passwords or keys. During authentication, the same transformation function is applied to the query and matched with the stored template in the transformed domain. (See below Figure 1.5)
- Biometric cryptosystems attempt to obtain error correcting information from the biometric features (with or without use of external key) that is known as helper data. The helper or auxiliary data does not reveal significant information about the biometric or the key. Error correcting codes are normally used in these systems to recover the enrolled biometric features or the key given the query biometric.(See below Figure 1.6)
- These two approaches can also be combined to consolidate their advantages. One way to combine them is to use a transformed template as the input to a biometric cryptosystem. Another possibility is to transform the helper data in a biometric cryptosystem using a homomorphic encryption scheme. (See below Figure 1.7)

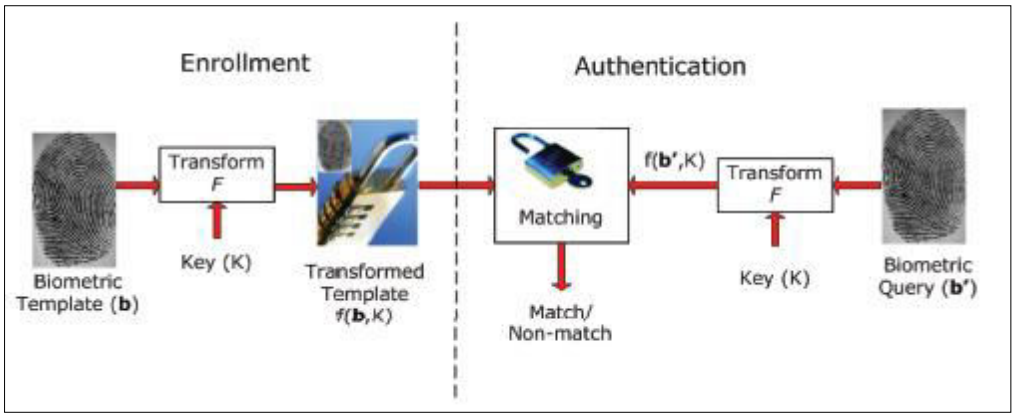


Figure 1.5: Schematic diagrams for Template Transformation approach

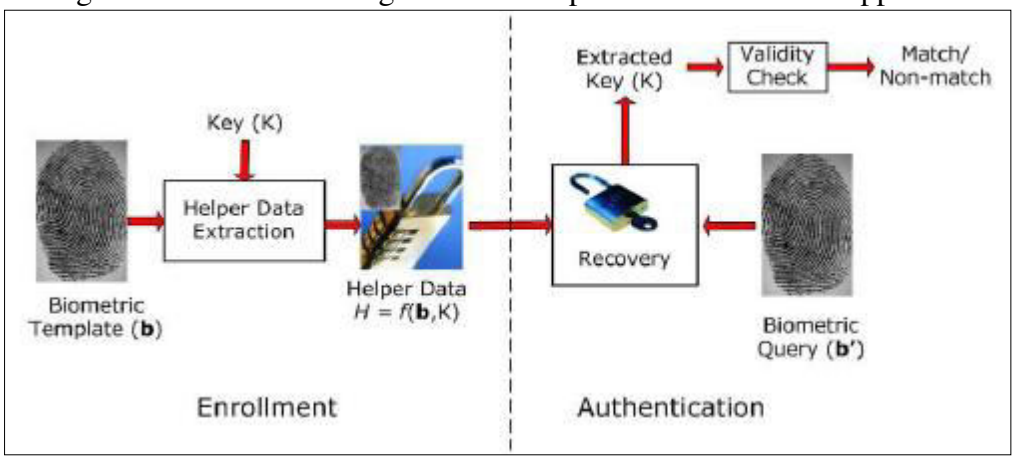


Figure 1.6: Schematic diagrams for Biometric Cryptosystem

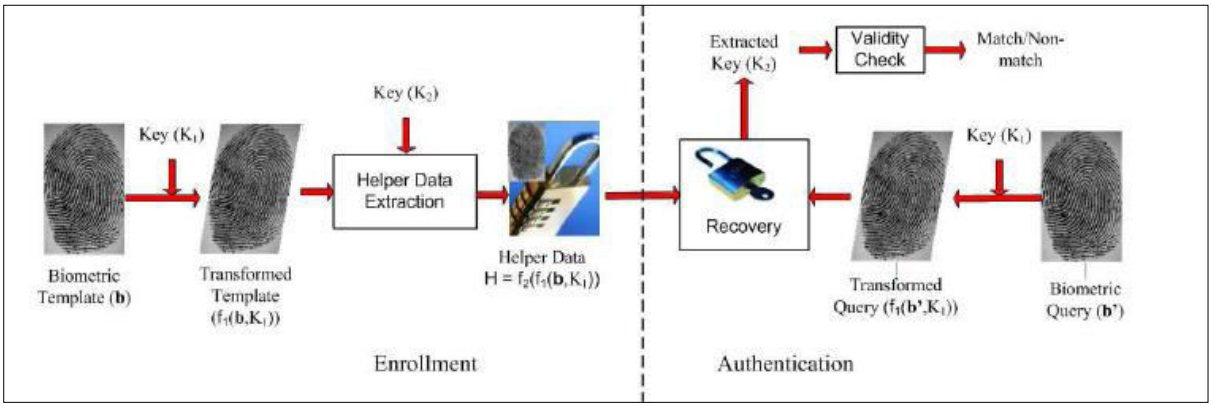


Figure 1.7: Schematic diagrams for Hybrid Bio-metric Cryptosystem.

5. Importance of study:

- The Security of multi-biometric templates is especially crucial as they contain information regarding multiple traits of the same subject. The leakage of any kind of template information to unauthorized individuals constitutes serious security and privacy risks, e.g. permanent tracking of subjects without consent or reconstruction of original biometric traits (e.g. fingerprints or iris textures) might become a realistic threat. Therefore, biometric template protection technologies have been developed in order to protect privacy and integrity of stored biometric data.

- By combining multiple sources of information, it is possible to improve systems biometric performance, increase population coverage, deter spoofing etc.
- Compared to conventional biometric systems based on a single biometric indicator, multiple sources of information, i.e. more biometric reference data, has to be stored for each subject registered with a multi-biometric system.
- Biometric template protection technologies offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level.

6. Proposed work Plan:

Year-wise Plan of work and targets to be achieved:

Activities	2016	2017		2018
	July to December	January to June	July to December	January to June
Study Research Problem, Collection of research paper and review, Synopsis preparation.				
Literature Review & Information gathering.				
Preliminary Analysis, Graphical representation and designing.				
Study models of Biometric Systems.				
Data Collection and Preprocessing.				
Main Experiment: Study, analyze and implement Biometric Template protection Tool.				
Test and setup different testing strategies.				
Conclusion and Future Directions.				
Pre-thesis evaluation.				
Summary and Final draft of thesis.				
PhD Thesis Writing & submission.				

Mr. Patil Pratap Paraji
Research Scholar

Dr. Jagtap Sudhir Baburao
Research Supervisor / Guide

7. References:

1. Abhishek Nagar, Karthik Nandakumar and Anil K. Jain, "Biometric Template Transformation: A Security Analysis", Proceedings SPIE, 7541, Media Forensics and Security II, January 2010.
2. Adler, "Can images be regenerated from biometric templates?" In Biometrics Consortium Conference, Arlington, VA, September 2003.
3. Adler, "Images can be regenerated from quantized biometric match score data," In Proceedings of Canadian Conference Electrical Computer Eng., pp. 469-472, Niagara Falls, Canada, May 2004.
4. Adler, "Vulnerabilities in Biometric Encryption Systems," In Audio- and Video- Based Biometric Person Authentication, pp. 1100-1109, 2005.
5. Christian Rathgeb and Christoph Busch, in book "New Trends and Developments in Biometrics", Chapter 8 named "Multi-Biometric Template Protection: Issues and Challenges " ISBN: 978-953-51-085-7 at http://dx.doi.org/10.5772/52152, Nov. 2012.
6. Christina-Angeliki Toli, Bart Preneel, "A Survey on Multimodal Biometrics and the Protection of Their Templates", IFIP International Federation for Information Processing 2015 J. Camenisch et al. (Eds.): Privacy and Identity 2014, pp. 169–184, 2015.
7. E. Srinivasa Reddy, and I. Ramesh Babu, "Performance of Iris Based Hard Fuzzy Vault," In Proceedings of IEEE 8th International conference on computers and Information technology workshops, pp. 248 - 253, 2008.
8. G. Karthi, M. Ezhilarasan, "Hybrid Multimodal Template Protection Technique Using Fuzzy Extractor And Random Projection" in International Journal of Research in Computer and Communication Technology, Vol 2, Issue 7, July-2013, ISSN(Online) 2278-5841, ISSN (Print) 2320-5156.
9. H. Ailisto, E. Vildjiounaite, M. Lindholm , and S.Mäkelä, "Soft biometrics combining body weight and fat measurements with fingerprint biometrics," Source Pattern Recognition Letters, ISSN:0167-8655, vol. 27, no. 5, pp. 325-334 , April 2006.
10. H. K. Jee, S.U. Jung , and J. H. Yoo, "Liveness detection for embedded face recognition system," International Journal of Biomedical Sciences," vol. 1, no. 4, pp. 235-238, 2006.
11. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," In Biometric Technology for Human Identification, vol. 5404 of Proceedings of SPIE, Orlando, Fla, USA, pp. 296-303, April 2004.
12. J. M. Williams, "Assurance in life / nation critical endeavors: Biometrics or ... biohazards?," In Proceedings of the 2002 workshop on New security paradigms, Virginia Beach, Virginia, pp. 97 - 107, 2002.
13. Jules, M. Sudan. "A Fuzzy Vault Scheme" In Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland p.408, 2002.
14. Juels, M. Wattenberg, " A Fuzzy Commitment Scheme," In G. Tsudik, editor, Sixth ACM Conference on Computer and Communications Security, pp. 28-36, ACM Press, 1999.
15. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, 2006.
16. K. Jain, and A. Ross, "Multi-biometric systems," Communications of the ACM," special issue on multimodal interfaces, vol. 47, no.1, pp. 34-40, January 2004.
17. K. Jain, and U. Uludag, "Hiding biometric data", Pattern Analysis and Machine

Intelligence, IEEE Transactions on vol. 25, no. 11, November 2003.
18. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security" EURASIP Journal on Advancing Signal Processing, special issue on Biometrics, pp. 1-17, January 2008.
19. K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating Liveness by face images and the structure tensor," In Proceedings of the 4th IEEE Workshop on Automatic Identification Advanced Technologies (AUTO ID '05), Buffalo, NY, USA, pp. 75-80, October 2005.
20. K. Nandakumar, A. Nagar and A. K. Jain, "Hardening Fingerprint Fuzzy Vault using Password," In Proceedings of 2nd International Conference on Biometrics, Seoul, South Korea, pp. 927-937, August 2007.
21. L. Nanni and A. Lumini, "A multi-modal method based on the competitors of FVC2004 and on Palm data combined with tokenized random numbers," Pattern Recognition Letters, vol.29, no.9, pp.1344-1350, July 2008.
22. L. Nanni, E. Maiorana, A. Lumini and P. Campisi, "Combining local, regional and global matchers for a template protected on-line signature verification system," Expert Systems with Applications, vol.37, no.5, pp.3676-3684, May 2010.
23. Li Chen, and Xiao-Long Zhang, "Feature-based image registration using bifurcation structures", available at http:/read.pudn.com/downloads153/sourcecode/graph /texture_ mapping/674198 /Registration/manuscript_registration.pdf.
24. M. G. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and Prevent misuse of biometric templates," in AVBPA, pp. 393-402, 2003.
25. N. K. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, ISSN: 0018-8670, vol. 40, no.3, pp. 614 - 634, March 2001.
26. N. Radha, S. Karthikeyan, "A Study on Biometric Template Security" In ICTACT Journal on Soft Computing, Issue: 01, pages 37-41, July 2010.
27. Nagar, K. NandaKumar, and A. K. Jain, "Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates," Pattern Recognition Letters vol. 31, no. 8, pp. 733-741, ISSN: 0167-865, June 2010.
28. O. T. Song, A. B. J. Teoh, and D. C. L. Ngo, "Application-specific key release scheme from biometrics," International Journal of Network Security," vol. 6, no. 2, pp. 127-133, 2008.
29. P. Tuyls, E. Verbitsky, T. Ignatenko, D. Schobben and T.H. Akkermans, "Privacy Protected Biometric Templates, Acoustic Ear Identification," Proceedings SPIE, Biometric Technology for Human Identification; Anil K. Jain, Nalini K. Ratha; Editors., vol. 5404, pp. 176-182 August 2004.
30. Parvathy ambalakat, "Security of Biometric Authentication System", in proceedings of 21st Computer Science Seminar, 2005, available at www.rh.edu/~rhb/cs_seminar_2005/SessionA1/ambalakat.pdf, 2005.
31. Praveer Tigga, Akash Wanjari, "A Survey on Template Protection Scheme for Multimodal Biometric System " in International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 4 Issue 7, July 2015
32. Ross, J. Shah, and A. K. Jain, "From Template to Image: Reconstructing Fingerprints from Minutiae Points," IEEE Transactions of Pattern Analysis and Machine Translation,

vol. 29, pp. 544-560, 2007.
33. S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a Liveness test in fingerprint devices," IEEE Transactions on Systems, Man and Cybernetics Part C, vol. 35, no. 3, pp. 335-343, 2005.
34. Shweta Malhotra, Chander Kant Verma , "A Hybrid Approach for Securing Biometric Template ", in International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013
35. Srinivasa Kumar Devi reddy, "Integrated approach for Automated Authentication based on Biometrics and Tools of Image Processing", in thesis submitted to Institute of Science and Technology, Jawaharlal Nehru Technological University, Hyderabad, June 2010.
36. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain., "Biometric Cryptosystems: Issues and Challenges," Proceedings of the IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol.92, no. 6, pp. 948-960, June 2004.
37. U. Waldmann, D. Scheuermann, and C. Eckert, "Protected transmission of biometric user Authentication data for oncard-matching," Proceedings of the 2004 ACM symposium on Applied computing, Nicosia, Cyprus, pp.425 - 430, March 2004.
38. V Evelyn Brindha, AM Natarajan, "Multi-Modal Biometric Template Security: Fingerprint and Palmprint Based Fuzzy Vault ", J Biom Biostat JBMBS, ISSN: 2155-6180, Volume 3, Issue 6, 2012.
39. V. S. Meenakshi, "Secure and Revocable Biometric template using Fuzzy Vault for Fingerprint, Iris and Retina", in Thesis submitted to Avinashi lingam Deemed University for Women, Coimbatore, and October 2010.
40. Y. C. Feng and P. C. Yuen," Protecting Face Biometric Data on Smartcard with Reed-Solomon Code," In Proceedings of CVPR Workshop on Privacy Research In Vision, New York, USA, pp. 29, June 2006.
41. Y. C. Feng, Pong C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," IEEE Transactions on Information Forensics and Security, vol.5, no.1, pp.103-117, March 2010.
42. Y. Wang, T. Tan, and A. K. Jain, "Combining face and iris biometrics for identity verification," In Proceedings of 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), J. Kittler and M. Nixon, Eds., vol. LNCS 2688, pp. 805-813, 2003.

#####